



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/991,506	11/16/2001	Tad Jarosinski	010147	7709

23696 7590 09/27/2005

Qualcomm, NC
5775 Morehouse Drive
San Diego, CA 92121

EXAMINER

BAUM, RONALD

ART UNIT PAPER NUMBER

2136

DATE MAILED: 09/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/991,506

Applicant(s)

JAROSINSKI ET AL.

Examiner

Ronald Baum

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-34 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-34 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. ____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. ____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>09152005</u> | 6) <input type="checkbox"/> Other: ____ |

RD

DETAILED ACTION

1. Claims 1- 34 are pending for examination.
2. Claims 1- 34 are rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1- 4,8-11,14-19,22-24,27-30 are rejected under 35 U.S.C. 102(b) as being anticipated by Dent et al, U.S. Patent 5,771,288.

4. As per claim 1; “A method for secure wireless communication using spread spectrum principles, comprising:

generating at least one pseudorandom number (PN) sequence [ABSTRACT, col. 3,lines 5-col. 28,line 5, whereas the ‘pseudo-randomly generated code key is used to select ...’, clearly encompasses the claimed limitations as broadly interpreted by the examiner];

encrypting the PN sequence to render an encrypted PN sequence [ABSTRACT, col. 3,lines 5-col. 28,line 5, whereas the ‘pseudo-randomly generated ciphering ...’, clearly encompasses the claimed limitations as broadly interpreted by the examiner]; and

using the encrypted PN sequence to spread a communication signal [ABSTRACT, col. 3,lines 5-col. 28,line 5, whereas the ‘spread spectrum ... CDMA ...’, clearly encompasses the claimed limitations as broadly interpreted by the examiner].”.

As per claim 14, this claim is the embodied software for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection; "A computer program product, comprising:

means for encrypting a PN sequence; and

means for providing the PN sequence to

a spread spectrum communication device for use thereof in

spreading or

despreading a communication signal."

As per claim 27, this claim is the 'receiving side' for the 'transmitting side' method claim 1 above, whereas the rejection of claim 1 clearly deals with both transmission and reception aspects of the 'pseudo-randomly generated code key is used to select ...' in 'spread spectrum ... CDMA ...', and is rejected for the same reasons provided for the claim 1 rejection; "A method for secure wireless communication using spread spectrum principles, comprising:

receiving at least one encryption sequence;

using the encryption sequence to

render an encrypted PN sequence; and

using the encrypted PN sequence to

despread a received spread spectrum signal to

render a despread signal."

Art Unit: 2136

5. Claim 2 *additionally recites* the limitation that; “The method of claim 1, wherein the communication signal is received from
- a data modulation component including
- a Walsh modulator.”.

The teachings of Dent et al suggest such limitations (ABSTRACT, col. 3, lines 5-col. 28, line 5, whereas the ‘spread spectrum ... CDMA [i.e., figures 6-9 and associated descriptions] ...’, clearly encompasses the claimed limitations as broadly interpreted by the examiner).

As per claim 28, this claim is the ‘receiving side’ for the ‘transmitting side’ method claim 2 above, whereas the rejection of claim 2 clearly deals with both transmission and reception aspects in ‘spread spectrum devices’, and is rejected for the same reasons provided for the claim 2 rejection; “The method of claim 27, wherein

the despread signal is sent to

a Walsh modulator.”.

6. Claim 3 *additionally recites* the limitation that; “The method of claim 1, wherein the PN sequence is encrypted by combining the PN sequence with
- at least one encryption sequence.”.

The teachings of Dent et al suggest such limitations (ABSTRACT, col. 3, lines 5-col. 28, line 5, whereas the ‘pseudo-randomly generated ciphering ... [i.e., figures 6-9 and associated descriptions]’, clearly encompasses the claimed limitations as broadly interpreted by the examiner).

As per claim 29, this claim is the 'receiving side' for the 'transmitting side' method claim 3 above, whereas the rejection of claim 3 clearly deals with both transmission and reception aspects in 'spread spectrum devices', and is rejected for the same reasons provided for the claim 3 rejection; "The method of claim 27, wherein

the PN sequence is encrypted by combining

the PN sequence with

at least one encryption sequence."

7. Claim 4 ***additionally recites*** the limitation that; "The method of claim 1, wherein one or more PN sequences are encrypted by combining

the PN sequences with

at least one encryption sequence."

The teachings of Dent et al suggest such limitations (ABSTRACT, col. 3, lines 5-col. 28, line 5, whereas the 'pseudo-randomly generated ciphering ... [i.e., figures 6-9 and associated descriptions]', and mask selection using cryptographic associated criteria, clearly encompasses the claimed limitations as broadly interpreted by the examiner).

As per claim 30, this claim is the 'receiving side' for the 'transmitting side' method claim 4 above, whereas the rejection of claim 4 clearly deals with both transmission and reception aspects in 'spread spectrum devices', and is rejected for the same reasons provided for the claim 4 rejection; "The method of claim 27, wherein

one or more PN sequences are encrypted by combining
the PN sequences with
at least two encryption sequences.”.

8. As per claim 8; this claim is the claims 1,2 expanded combination, and is rejected for the same reasons provided for the claims 2 rejection; “A wireless communication system, comprising:

at least one data modulation component

coding a communication signal for error correction to produce a coded signal,
interleaving bits in the coded signal to produce an interleaved coded signal to
reduce the effect of error bursts, and

modulating the interleaved coded signal using a Walsh function to produce a
Walsh-modulated interleaved coded signal [ABSTRACT, col. 3,lines 5-col. 28,line 5,
whereas the ‘spread spectrum ... CDMA (i.e., figures 6-9 and associated descriptions)
...’, clearly encompasses the claimed limitations as broadly interpreted by the examiner];
and

at least one carrier modulator for

spreading the Walsh-modulated interleaved coded signal with
a pseudorandom number (PN) sequence encrypted with
at least one encryption sequence.”.

As per claim 16; this claim is the intended use embodiment of claim 8 above, and is rejected for the same reasons provided for the claim 8 rejection (A recitation directed to the manner in which a claimed apparatus is *intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so perform* (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987)). The *prior art is replete with references disclosing generally electrically equivalent embodiments such as that implemented in the CDMA based cellular phone system of Dent.*); “A chip for use in a communication device, comprising:

at least one data modulation component including:

at least one channel coder receiving a signal for communication,

the channel coder coding

the signal for error correction to produce

a coded signal;

at least one bit interleaver coupled to

the channel coder for

interleaving bits in the coded signal to produce

an interleaved coded signal to reduce

the effect of error bursts;

at least one Walsh modulator coupled to

the bit interleaver and modulating the interleaved coded signal using a

Walsh function to produce

a Walsh-modulated interleaved coded signal; and

at least one carrier modulator for

spreading the Walsh-modulated interleaved coded signal with a
pseudorandom number (PN) sequence encrypted with
at least one encryption sequence.”.

As per claim 22, this claim is the ‘receiving side’ for the ‘transmitting side’ chip apparatus claim 16 above, whereas the rejection of claim 16 clearly deals with both transmission and reception aspects in ‘spread spectrum devices’, and is rejected for the same reasons provided for the claim 16 rejection; “A chip for use in a communication device, comprising:

at least one PN sequence generator

receiving at least one encryption sequence and

combining

the encryption sequence with

a PN sequence to establish a combined sequence;

at least one carrier demodulator

despreading a received spread spectrum communication signal using the
combined sequence to

render a despread signal; and

at least one data demodulation component coupled to the carrier demodulator to

Walsh-process the despread signal,

the demodulation component also

deinterleaving the signal to render a deinterleaved signal and
channel-demodulating the deinterleaved signal.”.

9. Claim 9 ***additionally recites*** the limitation that; “The system of claim 8, comprising
a PN generator
generating the PN sequence and
receiving the encryption sequence.”.

The teachings of Dent et al suggest such limitations (ABSTRACT, col. 3, lines 5-col. 28, line 5, whereas the ‘pseudo-randomly generated ciphering ... [i.e., figures 6-9 and associated descriptions]’, clearly encompasses the claimed limitations as broadly interpreted by the examiner).

As per claim 17; this claim is the intended use embodiment of claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection (A recitation directed to the manner in which a claimed apparatus is ***intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so perform*** (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987)). The *prior art is replete with references disclosing generally electrically equivalent embodiments such as that implemented in the CDMA based cellular phone system of Dent.*); “The chip of claim 16, comprising

- a PN generator
generating the PN sequence and
receiving the encryption sequence.”.
10. Claim 10 ***additionally recites*** the limitation that; “The system of claim 8, comprising

using two encryption sequences.”.

The teachings of Dent et al suggest such limitations (ABSTRACT, col. 3, lines 5-col. 28, line 5, whereas the ‘pseudo-randomly generated ciphering ... [i.e., figures 6-9 and associated descriptions]’, clearly encompasses the claimed limitations as broadly interpreted by the examiner).

As per claim 18; this claim is the intended use embodiment of claim 10 above, and is rejected for the same reasons provided for the claim 10 rejection (A recitation directed to the manner in which a claimed apparatus is *intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so perform* (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987)). The *prior art is replete with references disclosing generally electrically equivalent embodiments such as that implemented in the CDMA based cellular phone system of Dent.*); “The chip of claim 17, wherein

the encryption sequence is

a first sequence and

the PN generator receives

the first sequence and

a second encryption sequence,

the PN sequence being encrypted with

both encryption sequences.”.

11. Claim 23 *additionally recites* the limitation that; “The chip of claim 22, wherein

the encryption sequence is a first sequence and
the PN sequence generator receives
the first sequence and
a second encryption sequence.”.

The teachings of Dent et al suggest such limitations (ABSTRACT, col. 3, lines 5-col. 28, line 5, whereas the ‘pseudo-randomly generated ciphering ... [i.e., figures 6-9 and associated descriptions]’, clearly encompasses the claimed limitations as broadly interpreted by the examiner).

12. Claim 11 ***additionally recites*** the limitation that; “The system of claim 8, comprising an encryption sequence generator
generating the encryption sequence.”.

The teachings of Dent et al suggest such limitations (ABSTRACT, col. 3, lines 5-col. 28, line 5, whereas the ‘pseudo-randomly generated ciphering ... [i.e., figures 6-9 and associated descriptions]’, clearly encompasses the claimed limitations as broadly interpreted by the examiner).

As per claim 19; this claim is the intended use embodiment of claim 11 above, and is rejected for the same reasons provided for the claim 11 rejection (A recitation directed to the manner in which a claimed apparatus is ***intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so perform*** (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987)). The *prior art is replete with references*

Art Unit: 2136

disclosing generally electrically equivalent embodiments such as that implemented in the CDMA based cellular phone system of Dent.); “The chip of claim 16, comprising
an encryption sequence generator
generating the encryption sequence.”.

As per claim 24; this claim is the intended use embodiment of claim 16 above, and is rejected for the same reasons provided for the claim 16 rejection (A recitation directed to the manner in which a claimed apparatus is *intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so perform* (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987)). The *prior art is replete with references disclosing generally electrically equivalent embodiments such as that implemented in the CDMA based cellular phone system of Dent.); “The chip of claim 23, comprising*
an encryption sequence generator
generating the encryption sequence.”.

13. Claim 15 *additionally recites* the limitation that; “The product of claim 14, wherein the communication device uses
CDMA principles.”.

The teachings of Dent et al suggest such limitations (ABSTRACT, col. 3, lines 5-col. 28, line 5, whereas the ‘spread spectrum ... CDMA (i.e., figures 6-9 and associated descriptions) ...’, clearly encompasses the claimed limitations as broadly interpreted by the examiner).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 5-7, and 10,12-13, and 20-21, and 25-26, and 31-34 are rejected under 35

U.S.C. 103(a) as being unpatentable over Dent et al, U.S. Patent 5,771,288 as applied to claims 1,8,16,22,27, respectively above, and further in view of DeBellis et al, U.S. Patent 6,044,388.

14. Claim 5 ***additionally recites*** the limitation that; "The method of claim 3, wherein the encryption sequence is generated by

a DES or

triple-DES encryption."
15. Claim 6 ***additionally recites*** the limitation that; "The method of claim 5, wherein the DES or triple-DES encryption receives input including

at least one multi-bit key and

at least one time varying input."
16. Claim 7 ***additionally recites*** the limitation that; "The method of claim 6, wherein the key is periodically refreshed."

Art Unit: 2136

17. Claim 12 *additionally recites* the limitation that; “The system of claim 11, wherein the encryption sequence generator includes

a DES or

triple-DES encryption.”.
18. Claim 13 *additionally recites* the limitation that; “The system of claim 11, wherein the encryption sequence generator periodically

receives refresh keys useful in

generating the encryption sequence.”.
19. Claim 20 *additionally recites* the limitation that; “The chip of claim 19, wherein the encryption sequence generator includes

a DES or

triple-DES encryption.”.
20. Claim 21 *additionally recites* the limitation that; “The chip of claim 19, wherein the encryption sequence generator periodically

receives refresh keys useful in

generating the encryption sequence.”.
21. Claim 25 *additionally recites* the limitation that; “The chip of claim 24, wherein the encryption sequence generator includes

a DES or
triple-DES encryption.”.

22. Claim 26 ***additionally recites*** the limitation that; “The chip of claim 24, wherein the encryption sequence generator periodically receives refresh keys useful in generating the encryption sequence.”.
23. Claim 31 ***additionally recites*** the limitation that; “The method of claim 29, wherein the encryption sequence is generated by a DES or triple-DES encryption.”.
24. Claim 32 ***additionally recites*** the limitation that; “The method of claim 31, wherein the DES or triple-DES encryption receives input including at least one multi-bit key and at least one varying input.”.
25. Claim 33 ***additionally recites*** the limitation that; “The method of claim 32, wherein the key is periodically refreshed.”.
26. Claim 34 ***additionally recites*** the limitation that; “The method of claim 32, wherein

Art Unit: 2136

the varying input is

at least one long code state.”.

The teachings of Dent et al suggest the base claims limitations (see “As per claim 1..., As per claim 8..., 14..., 16..., 22..., 27...” paragraphs above) *without explicitly teaching* of the use of “... encryption sequence ... DES or triple-DES encryption ... least one multi-bit key ... periodically refreshed ... one long code state”, as a form of cryptographic encryption/pseudo-random number altering functionality per se.

DeBellis et al, teaches (i.e., col. 1, lines 15-col. 6, line 5) of generating pseudo-random numbers using cryptographic constructs (i.e., DES and triple DES). The DeBellis et al invention also clearly encompasses the cryptographic key security aspects associated with the applicants' communications insofar as generating said pseudo-random numbers using cryptographic constructs uses generated and entered/provided multi-bit key data; clearly security aspects associated with the applicants' claimed invention.

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the CDMA spread spectrum communications apparatus and method utilizing pseudo-random spread/dispreading criteria, with the DeBellis et al teachings of actual generation of such utilizing cryptographic constructs (i.e., DES and triple DES), in order to provide a less deterministic quality to the Dent et al mask selection, etc.

Such motivation to combine would clearly encompass the need to allow a higher degree of randomness (i.e., DeBellis et al col. 1, lines 15-col. 3, line 10).

Conclusion

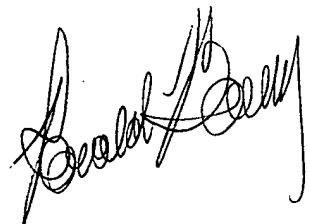

27. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner



Primary Examiner
AU 2131
9/23/05